Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

02-12-2025:

bpost slachtoffer van Tridentlocker ransomwareaanval

bpost, een Belgisch bedrijf actief in de postsector, is slachtoffer geworden van een ransomwareaanval door de Tridentlocker ransomwaregroep. De aanval werd ontdekt op 1 december 2025 en heeft invloed op de werking van het bedrijf, dat verantwoordelijk is voor de sortering, bezorging en het transport van postdiensten zowel lokaal als internationaal. bpost biedt ook elektronische communicatie, financiële transacties en andere verwante diensten aan. Het bedrijf opereert voornamelijk in de postsector en biedt e-commerce en pakketlogistiek aan in Europa, Noord-Amerika en Azië. De aanval werd op 1 december 2025 geconstateerd.

Mogelijk datalek bij KPN

Op 1 december 2025 werd melding gemaakt van een mogelijk datalek bij het Nederlandse telecombedrijf KPN N.V. Er zouden gegevens van het bedrijf zijn gecompromitteerd, maar de specifieke details van het incident zijn nog onduidelijk. Er is geen informatie verstrekt over de aard van het lek of de omvang van de blootgestelde data. Het is op dit moment niet bevestigd of de aanval al dan niet te maken heeft met een verkoop van de gestolen gegevens.

KPN heeft nog geen officiële verklaring afgelegd over het incident, en het is onduidelijk of de getroffen data betrekking heeft op persoonlijke klantinformatie of andere bedrijfsgegevens. Gezien de gevoeligheid van de gegevens die telecombedrijven beheren, zoals klantinformatie en communicatiegeschiedenis, zouden de gevolgen van een dergelijk datalek ernstig kunnen zijn. Het bedrijf en de relevante autoriteiten zullen waarschijnlijk nader onderzoek doen naar de toedracht van het incident.

Omdat het incident nog niet officieel bevestigd is, blijven de details voorlopig onduidelijk. Het is belangrijk om deze situatie te blijven volgen voor verdere updates.

NATO overweegt proactieve reactie op hybride aanvallen van Rusland, inclusief cyberaanvallen

NATO overweegt een meer proactieve benadering in reactie op de steeds intensievere hybride aanvallen van Rusland. Deze aanvallen omvatten onder andere

cyberaanvallen, sabotage-operaties en schendingen van het luchtruim. NATO-functionarissen hebben zelfs de mogelijkheid van een zogenaamde "preventieve aanval" op Russische doelwitten in overweging genomen.

Admiral Giuseppe Cavo Dragone, voorzitter van de militaire commissie van NATO, verklaarde in een interview met de Financial Times dat de alliantie haar traditionele reactieve houding heroverweegt, nu Europa wordt geconfronteerd met een toename van hybride incidenten die aan Rusland worden toegeschreven. Recente gevallen omvatten het doorsnijden van onderzeese kabels in de Baltische Zee, grootschalige cyberinbreuken over het continent en drone-activiteit nabij de grenzen van bondgenoten.

Dragone benadrukte dat hoewel een offensieve cyberreactie de eenvoudigste optie zou zijn, gezien veel lidstaten over dergelijke capaciteiten beschikken, het reageren op fysieke sabotage of drone-inbraken complexer zou zijn. Hij stelde dat een "preventieve aanval" onder bepaalde omstandigheden als een defensieve actie kan worden beschouwd, hoewel dit verder gaat dan de gebruikelijke manier van denken en handelen binnen NATO.

De zorgen over een te passieve benadering worden gedeeld door diplomaten, vooral uit Oost-Europa, die pleiten voor maatregelen die Rusland kosten zouden opleggen. Zij stellen dat als NATO alleen reactief blijft, Rusland wordt uitgenodigd om door te gaan met aanvallen. Tegelijkertijd wijst NATO op het succes van de operatie Baltic Sentry, die werd opgezet om vitale onderwaterinfrastructuur te beschermen. Deze gezamenlijke maritieme en luchtaanvallen hebben herhaling van de kabeldoorsnijdingsincidenten die in 2023 en 2024 plaatsvonden, voorkomen.

APT36 gebruikt Python-gebaseerde ELF-malware om overheidsinstanties te targeten

De hacker-groep APT36, die wordt geassocieerd met Pakistan en ook wel bekend is onder de naam Transparent Tribe, heeft een geavanceerde cyberespionagecampagne opgezet gericht op Indiase overheidsinstanties. Deze campagne maakt gebruik van nieuwe, Python-gebaseerde ELF-malware, wat een significante stap vooruit betekent in de capaciteiten van de groep. De groep heeft een verfijnde aanvalsmethode ontwikkeld die specifiek is aangepast voor Linux-besturingssystemen, waarmee ze hun aanvallen kunnen uitbreiden naar een nieuw platform dat veel wordt gebruikt door de Indiase overheid.

De aanval werd uitgevoerd via spear-phishing e-mails, die wapens bevatten in de vorm van schadelijke Linux-snelkoppelingbestanden. Deze bestanden werden zodanig ontworpen dat, wanneer ze werden geopend, de malware in de achtergrond werd gedownload en uitgevoerd zonder dat de gebruiker zich bewust was van de infectie. De malware werd vervolgens geïnstalleerd via een complexe, meerlagige aanvalsmethode die de aanvallers in staat stelde hun aanwezigheid geheim te houden en tegelijkertijd permanente toegang te verkrijgen tot kritieke infrastructuur.

De keuze van APT36 om over te schakelen van Windows naar Linux markeert een strategische wijziging in hun werkwijze. Hoewel de groep eerder vooral gericht was op Windows-systemen, toont deze nieuwe campagne aan dat ze zich nu ook richten op het BOSS-besturingssysteem, dat veelvuldig wordt ingezet binnen Indiase overheidsorganisaties. Dit wijst op een evolutie van hun operationele doctrines, waarbij meerdere platformen worden benut om de effectiviteit van hun aanvallen te vergroten.

De malware maakt gebruik van .desktop-bestanden om de schadelijke payload te verbergen en zo traditionele beveiligingsmaatregelen te omzeilen. Het bestand wordt gepresenteerd als een legitiem Linux-bestand, maar bevat verborgen commando's die de malware naar het systeem brengen. De malware zelf is een krachtige tool voor het verkrijgen van op afstand toegang, het uitvoeren van willekeurige commando's, het maken van schermafbeeldingen en het exfiltreren van data. Door gebruik te maken van systemd-gebruikerservices kan de malware zichzelf persistent maken, zodat deze blijft draaien na herstarts van het systeem.

De malware werd verspreid via phishingcampagnes die gebruik maakten van onlangs geregistreerde domeinen en gecompromitteerde servers in verschillende landen. De specifieke domeinen en IP-adressen die werden gebruikt om de payload te leveren, wijzen op een goed geplande en gecoördineerde aanval. De Indiase overheidsinstanties worden geadviseerd om onmiddellijk beveiligingsmaatregelen te versterken, zoals verbeterde e-mailbeveiliging en strikte endpointbeveiliging, om deze voortdurende dreiging te kunnen afweren.

OpenAI Codex CLI kwetsbaarheid: Command injection risico via projectconfiguratie

Een nieuwe kwetsbaarheid in de OpenAI Codex CLI is ontdekt, waarbij een aanvaller misbruik kan maken van project-specifieke configuratiebestanden om willekeurige

commando's uit te voeren. Codex CLI, een tool die bedoeld is om de ontwikkelworkflow te ondersteunen met AI-ondersteunde redenering en interactie via de commandoregel, heeft een probleem in de manier waarop het projectgebonden configuratiebestanden verwerkt.

Tijdens tests werd ontdekt dat Codex CLI project-specifieke configuraties, zoals .env-bestanden en de bijbehorende ./.codex/config.toml, automatisch laadt en uitvoert wanneer het project wordt uitgevoerd. Dit betekent dat als een ontwikkelaar een repository met een besmet .env-bestand en een kwaadaardige config.toml met MCP-serverinstellingen kloneert, het systeem ongevraagd commando's uitvoert bij het opstarten van Codex. Er is geen validatie of goedkeuring nodig van de gebruiker, waardoor aanvallers de mogelijkheid hebben om schadelijke code uit te voeren zonder dat de ontwikkelaar het merkt.

De kwetsbaarheid stelt een aanvaller in staat om op verschillende manieren toegang te krijgen. Zo kan een aanvaller een reverse shell in de configuratie plaatsen, waardoor ze persistente toegang verkrijgen tot het systeem van een ontwikkelaar die de besmette repository kloneert en Codex uitvoert. Dit creëert een achterdeur die elke keer dat Codex wordt uitgevoerd, opnieuw kan worden geactiveerd, wat het mogelijk maakt om gegevens te stelen, wachtwoorden te exfiltreren of verdere aanvallen uit te voeren.

De kwetsbaarheid werd op 7 augustus 2025 aan OpenAI gemeld, waarna op 20 augustus 2025 een patch werd uitgebracht in versie 0.23.0 van Codex CLI. Deze patch voorkomt dat de tool .env-bestanden zonder verdere goedkeuring kan gebruiken om de CODEX_HOME naar een projectmap te leiden. Gebruikers wordt dringend geadviseerd om Codex CLI bij te werken naar versie 0.23.0 of hoger om zich te beschermen tegen deze kwetsbaarheid.

Officiële versies van SmartTube-app geïnfecteerd met malware

Verschillende officiële versies van de SmartTube-app, een populaire mediaspeler voor Android-tv's en tv-boxes, zijn recent besmet geraakt met malware. Dit meldt de ontwikkelaar aan AFTVnews. Als gevolg van de besmetting werd de app door zowel Amazon als Google verwijderd van de Android-televisies. Aanvankelijk gaf de ontwikkelaar aan dat de digitale certificaten van de app waren gecompromitteerd, wat de basis vormde voor de infectie.

De malware-infectie bleek echter te komen door een besmetting van het systeem dat gebruikt wordt voor het creëren van de SmartTube APK-bestanden. Het is nog niet bekend hoe dit systeem precies besmet raakte, en het blijft onduidelijk welke versie van de app als eerste geïnfecteerd was. Volgens AFTVnews zouden de infecties begin november zijn begonnen. De malware heeft als doel om gegevens van besmette systemen terug te sturen naar de aanvallers en kan bovendien aanvullende opdrachten van de aanvallers uitvoeren.

In reactie op de besmetting heeft de ontwikkelaar een nieuwe versie van de app, versie 30.56, uitgebracht, met een nieuwe digitale handtekening om de infectie te verhelpen. Gebruikers wordt geadviseerd om de app bij te werken naar deze nieuwe versie om verdere risico's te vermijden.

Nieuwe Albiriox MaaS-malware richt zich op 400+ apps voor fraude en schermcontrole op Android-apparaten

Albiriox is een nieuwe Android-malware die wordt aangeboden via een Malware-as-a-Service (MaaS)-model en zich richt op financiële en cryptocurrency-apps. De malware biedt een breed scala aan functies voor on-device fraude (ODF), schermmanipulatie en real-time interactie met geïnfecteerde apparaten. De malware bevat een hardcoded lijst van meer dan 400 apps, waaronder bankapps, fintech, betalingsverwerkers, cryptocurrency-exchanges, digitale portefeuilles en handelsplatformen.

De verspreiding van Albiriox gebeurt via droppers die worden verspreid door middel van social engineering-lures en verpakt zijn om statische detectie te omzeilen. De malware werd aanvankelijk in september 2025 geadverteerd tijdens een beperkte wervingsfase, maar schakelde een maand later over naar een MaaS-aanbod. Het lijkt erop dat de dreigingsactoren Russischsprekend zijn, gebaseerd op hun activiteiten op cybercrime-forums, linguïstische patronen en de gebruikte infrastructuur.

De malware biedt een aangepaste builder aan voor klanten, die claimt samen te werken met een derde partij crypting-service genaamd Golden Crypt, bedoeld om antivirussoftware en mobiele beveiligingsoplossingen te omzeilen. Het doel van de aanvallen is om de controle over mobiele apparaten te verkrijgen en frauduleuze handelingen uit te voeren, terwijl het onder de radar blijft.

Een van de campagnes richtte zich specifiek op Oostenrijkse slachtoffers, waarbij Duitse social engineering-lures en SMS-berichten werden gebruikt om slachtoffers naar valse Google Play Store-pagina's te leiden. Wanneer gebruikers op de "Installeren"-knop van de vervalste app klikten, werden ze besmet met de malware. De geïnfecteerde app vroeg gebruikers om machtigingen om apps te installeren, die vervolgens de daadwerkelijke malware deployeerde.

Albiriox maakt gebruik van een onbeveiligde TCP-socketverbinding voor de command-and-control (C2)-communicatie, waardoor de dreigingsactoren verschillende opdrachten kunnen uitvoeren, zoals het op afstand bedienen van het apparaat met Virtual Network Computing (VNC), het verzamelen van gevoelige informatie, het tonen van zwarte of lege schermen en het aanpassen van het volume voor operationele stealth. Het gebruikt Android’s toegankelijkheidsservices om de scherminhoud te streamen en voorkomt zo beperkingen die normaal door Android’s FLAG_SECURE-beveiliging worden opgelegd.

Deze malware ondersteunt ook overlay-aanvallen tegen de vooraf geconfigureerde apps op de lijst, wat leidt tot het stelen van inloggegevens. Daarnaast kan Albiriox overgangen naar vervalste schermen simuleren, zoals een systeemupdate, zodat kwaadaardige activiteiten in de achtergrond kunnen plaatsvinden zonder aandacht te trekken.

De ontdekking van Albiriox valt samen met de opkomst van een andere Android MaaS-tool, genaamd RadzaRat, die zich voordoet als een legitieme bestandsbeheerder maar in werkelijkheid uitgebreide surveillance- en remote control-mogelijkheden biedt. Deze tools benadrukken de toenemende toegankelijkheid en "democratisering" van cybercriminaliteit, waarbij aanvallers met minimale technische kennis steeds effectievere kwaadaardige software kunnen inzetten.

Browser-extensies met miljoenen installaties na jaren voorzien van malware

Recent onderzoek heeft aangetoond dat verschillende browser-extensies, die oorspronkelijk in 2018 en 2019 werden gelanceerd, na verloop van tijd voorzien zijn van malware. Deze extensies zijn miljoenen keren gedownload en geïnstalleerd, wat aangeeft hoe kwetsbaar gebruikers kunnen zijn voor dergelijke aanvallen. De extensies, die onder andere beschikbaar waren voor Google Chrome en Microsoft Edge, kregen de zogenaamde "Featured" en "Verified" status, wat hun betrouwbaarheid suggereerde.

Vijf van de extensies, die samen 300.000 installaties hadden, werden via een malafide update voorzien van malware. Deze malware maakte gebruik van een "remote code execution framework" dat JavaScript-bestanden binnen de browser uitvoerde. Daarnaast verzamelde de malware informatie over de bezochte websites en stuurde die gegevens naar de aanvallers. Een van de besmette extensies was Clean Master, die 200.000 keer was geïnstalleerd en werd gepromoot als een opschoon- en optimalisatie-extensie.

Daarnaast ontdekten de onderzoekers een andere reeks extensies van dezelfde ontwikkelaar, die meer dan vier miljoen keer waren geïnstalleerd. Een daarvan was WeTab, met drie miljoen installaties. Deze extensies verzamelde real-time gegevens over bezochte websites, zoekopdrachten en andere gebruikersinformatie, wat duidt op spyware-activiteiten. Het automatische updateproces, dat doorgaans bedoeld is om gebruikers te beschermen, werd in dit geval misbruikt om de malware ongemerkt te installeren.

Hoewel Google de betreffende extensies inmiddels heeft verwijderd uit de Chrome Web Store, zijn ze nog steeds beschikbaar in de extensie-store van Microsoft Edge. Dit benadrukt de risico's van het vertrouwen op automatische updates in een systeem dat door kwaadwillenden kan worden misbruikt.

TangleCrypt malware-packer ontwijkt EDR door ABYSSWORKER-driver

TangleCrypt is een nieuw ontdekt malware-packer voor Windows die specifiek is ontworpen om ransomware-aanvallen te vergemakkelijken door Endpoint Detection and Response (EDR)-oplossingen te omzeilen. Deze malware, die voor het eerst werd waargenomen tijdens een ransomware-incident in september 2025, maakt gebruik van meerdere lagen van codering, compressie en encryptie om zijn kwaadaardige payloads te verbergen, waardoor traditionele beveiligingstools moeite hebben met het detecteren van het daadwerkelijke malwarebestand.

TangleCrypt verpakt de kwaadaardige payloads door middel van een combinatie van base64-codering, LZ78-compressie en XOR-encryptie. Het resulterende uitvoerbare bestand wordt opgeslagen in de PE-bronnen en is hierdoor voor beveiligingstools moeilijk te analyseren. De malware maakt gebruik van het ABYSSWORKER-driver, een programma dat is ontworpen om beveiligingsprocessen van de geïnfecteerde systemen geforceerd te beëindigen voordat de ransomware daadwerkelijk wordt ingezet.

Dit malware-pakket maakt gebruik van dynamische importoplossing en string-encryptie om zowel statische als dynamische analyse te bemoeilijken. Hoewel dergelijke technieken gebruikelijk zijn in de malwarewereld, is de implementatie van TangleCrypt niet bijzonder geavanceerd, wat betekent dat ervaren analisten in staat zijn om het handmatig uit te pakken.

Het payload-executiemechanisme van TangleCrypt ondersteunt twee methoden om de kwaadaardige code uit te voeren. De eerste methode decrypteert en voert de payload uit binnen hetzelfde procesgeheugen. De tweede methode maakt een tijdelijk child-process aan, waar de gedecodeerde payload in wordt geschreven, waarna de uitvoering van het child-process wordt hervat. Na succesvolle decryptie en uitvoering van de payload, controleert het systeem of het over beheerdersrechten beschikt. Indien dat het geval is, wordt de ABYSSWORKER-driver geregistreerd en worden vooraf gedefinieerde beveiligingsprocessen gedood.

De TangleCrypt malware maakt het voor slachtoffers gemakkelijker om de ransomware te verspreiden, omdat het de verdedigingen van een systeem uitschakelt voordat de encryptie van bestanden begint. Deze ontdekking benadrukt de voortdurende evolutie van ransomware en de manieren waarop kwaadwillende actoren technologie gebruiken om beveiligingsmaatregelen te ontwijken.

Europol haalt cryptomixer offline en neemt 25 miljoen euro aan crypto in beslag

Europol heeft in samenwerking met de Duitse en Zwitserse politie een cryptomixer offline gehaald, waarbij 25 miljoen euro aan cryptovaluta in beslag werd genomen. De actie vond plaats nadat de cryptomixer, die zichzelf de naam Cryptomixer had gegeven, werd beschuldigd van betrokkenheid bij witwaspraktijken en het faciliteren van cybercriminaliteit. De in beslag genomen goederen omvatten niet alleen de cryptovaluta, maar ook een domeinnaam en drie servers met daarop twaalf terabyte aan data.

Cryptomixers spelen een belangrijke rol in het verhullen van de herkomst en bestemming van cryptovaluta. Gebruikers kunnen hun cryptovaluta mengen met die van anderen, waardoor het moeilijker wordt om de oorsprong van de digitale valuta te traceren, die normaal gesproken via de blockchain te volgen is. Hoewel voorstanders van cryptomixers beweren dat ze legitieme doeleinden dienen, zoals het beschermen van de privacy van gebruikers, wordt de dienst in dit geval gezien

als een middel voor het witwassen van geld en het faciliteren van cybercriminaliteit, zoals het ontvangen van losgeldbetalingen in ransomware-aanvallen.

Europol meldt dat er sinds de oprichting van Cryptomixer in 2016 ongeveer 1,3 miljard euro aan bitcoin via de dienst is gemixt. De beschuldigingen richten zich onder andere op de betrokkenheid bij betalingen voor ransomware-aanvallen. Op dit moment heeft Europol geen details verstrekt over eventuele arrestaties van personen die verantwoordelijk zouden zijn voor de cryptomixer.

Man krijgt 3 jaar cel voor het oplichten van ICS-klanten via phishingaanval

Een 20-jarige man is door de rechter veroordeeld tot een gevangenisstraf van drie jaar, waarvan zes maanden voorwaardelijk, voor het oplichten van meer dan vijftig klanten van de creditcardmaatschappij ICS via een phishingaanval. De man stuurde zogenaamde "sms-bommen" naar talloze mensen. Deze berichten leken afkomstig van ICS en verwezen naar een phishingsite die slachtoffers vroeg om persoonlijke gegevens en creditcardinformatie in te vullen.

Met de verkregen gegevens bestelde de man verschillende producten, waaronder elektronica zoals laptops en telefoons. Opmerkelijk is dat hij ook grote hoeveelheden vlees bestelde, die later in zijn vriezer werden aangetroffen. In sommige gevallen gaf hij valse afleveradressen op, waaronder dat van een buurjongen. Verder ontdekte de politie dat de man in bezit was van meerdere lijsten met potentiële slachtoffers.

De rechter sprak van een geraffineerde en systematische werkwijze waarbij de verdachte de slachtoffers erin slaagde te laten geloven dat zij daadwerkelijk contact hadden met hun creditcardmaatschappij. Dit gaf de verdachte volledige toegang tot de creditcards van de slachtoffers, die hierdoor aanzienlijke schade opliepen. Naast de gevangenisstraf moet de man ook verschillende slachtoffers vergoeden, waaronder ICS, voor een bedrag van 35.000 euro.

Nieuw landelijk systeem maakt heimelijke inzage in patiëntendossiers mogelijk

Een nieuw landelijk systeem voor het elektronisch delen van medische gegevens, genaamd Mitz, maakt het mogelijk voor zorgverleners om heimelijk inzage te krijgen in patiëntendossiers. Het systeem is ontworpen om patiënten via DigiD de controle te geven over welke zorgverleners hun medische gegevens mogen delen. Het systeem bevat echter enkele zorgwekkende beveiligingsrisico’s.

Mitz heeft als doel om medische gegevens efficiënt te delen tussen zorgverleners, maar de implementatie van dit systeem is omstreden. De toestemming die patiënten geven voor het delen van hun gegevens is vaak te algemeen en moeilijk te controleren. Zo kunnen zorgverleners zonder de patiënt aanwezig te hebben, de toestemming aanpassen, wat de privacy van de patiënt in gevaar brengt. Dit geldt ook voor de zogenaamde 'Samen naar Mijn Mitz'-knop, waarmee zorgverleners namens niet-digitale patiënten toestemming kunnen regelen, zonder extra inlogprocedures.

Kritiek is er ook op de centrale opzet van het systeem. Mitz wordt vergeleken met het Landelijk Elektronisch Patiëntendossier (EPD) uit 2011, dat vanwege soortgelijke problemen werd stopgezet. De kritiek richt zich vooral op het gebrek aan granulariteit in de toestemming van de patiënt en het ontbreken van voldoende bescherming tegen misbruik. Privacyorganisaties wijzen op de grotere risico’s die verbonden zijn aan de opslag van gegevens in een centraal systeem.

Ondanks deze zorgen wordt er aan het systeem verder gewerkt en wordt verwacht dat het eind volgend jaar breed geïmplementeerd zal worden. Het ministerie van Volksgezondheid en de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ), die het systeem beheert, erkennen de risico’s, maar stellen dat de voordelen van het systeem opwegen tegen de nadelen. De Autoriteit Persoonsgegevens volgt de ontwikkelingen op de voet.

Zuid-Koreaanse webshop Coupang lekt gegevens van 33 miljoen klanten

De Zuid-Koreaanse webshop Coupang, die vaak wordt aangeduid als de 'Amazon van Azië', heeft de gegevens van meer dan 33 miljoen klanten gelekt. Het betreft onder andere namen, e-mailadressen, telefoonnummers, bezorgadressen en bestelgeschiedenis. Dit datalek heeft een groot deel van de Zuid-Koreaanse bevolking getroffen, aangezien het land bijna 52 miljoen inwoners telt, wat betekent dat het lek ongeveer 65 procent van de bevolking raakt.

De aanval werd mogelijk door een kwetsbaarheid in de authenticatie van de servers van Coupang, die door de aanvaller werd misbruikt. Dit werd bevestigd door de Zuid-Koreaanse minister Bae Kyung-hoon van Wetenschap. Aanvankelijk meldde Coupang dat slechts 4500 klanten betroffen waren, maar na nader onderzoek werd dit aantal bijgesteld naar 33,7 miljoen. De Zuid-Koreaanse politie heeft een verdachte in beeld die vermoedelijk het land heeft verlaten. Dit incident volgt op een

vergelijkbaar datalek bij telecomgigant SK Telecom eerder dit jaar, waarbij gegevens van 25 miljoen klanten werden gestolen.

Overstap Belastingdienst naar M365 maakt overheid afhankelijker van VS

De overstap van de Belastingdienst naar Microsoft 365 heeft geleid tot zorgen over de toenemende afhankelijkheid van de overheid van de Verenigde Staten. Demissionair staatssecretaris Heijnen van Financiën erkende in reactie op Kamervragen van de politieke partijen D66, GroenLinks-PvdA en NSC dat de overstap de afhankelijkheid van de VS vergroot. Deze partijen hadden vragen gesteld over de impact van de overstap op de relatie tussen Nederland en de VS, met name over de toegang van Amerikaanse autoriteiten tot persoonsgegevens van Nederlandse burgers.

Heijnen benadrukte dat de Amerikaanse cloudwetgeving de leverancier, Microsoft, kan verplichten om gegevens te verstrekken, wat betekent dat het niet volledig uitgesloten kan worden dat Amerikaanse opsporingsdiensten toegang krijgen tot dergelijke gegevens. De CLOUD Act maakt het mogelijk dat de Amerikaanse overheid, inclusief veiligheidsdiensten, toegang kan krijgen tot persoonlijke informatie, zelfs als deze buiten de VS is opgeslagen.

De staatssecretaris legde uit dat de Belastingdienst verschillende alternatieve scenario’s heeft onderzocht, maar dat er op dit moment geen geschikt alternatief is voor de overstap naar Microsoft 365. Er wordt verwacht dat een alternatief pas over twee tot drie jaar beschikbaar zal zijn. Desondanks heeft de Belastingdienst een uitgebreide risicoanalyse uitgevoerd en aanvullende afspraken met de leverancier gemaakt om de risico’s te beperken. Heijnen liet weten dat de risicoanalyse en de exitstrategie vertrouwelijk blijven en alleen ter inzage aan de Kamerleden worden verstrekt.